BAREILLY INTERNATIONAL UNIVERSITY,BAREILLY

Effectiveness of online course on knowledge and perception regarding cyber safety among Nursing Students:Mixed method study.

By

Ms.Anitha.P

Protocol of Thesis to be submitted to the Bareilly International University, Bareilly for the partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

(Nursing)

(Batch 2018-2021)

FACULTY OF NURSING

Certificate bythe Supervisor

Facultyof Nursing

(Affiliated to Bareilly International University, Bareilly)

This is to certify that the facilities for the research workentitled **"effectiveness of online course on knowledge and perception regarding cyber safety among Nursing students: mixed method study"** allotted to **Ms. ANITHA .P** under my direct supervision and guidance do exist in Faculty of Nursing, Bareilly.

I will ensure the authenticity of the thesis protocol topic and research methodology which conforms to the standards of Bareilly International University.

Supervisor

Signature 28/4/19

Name with Degree: Dr. *Prema .P*

Faculty of Nursing

Faculty of Nursing

(Affiliated to Bareilly International University, Bareilly)

DECLARATION BY THE CANDIDATE

I hereby declare that this thesis protocol entitled "effectiveness of online course on knowledge and perception regarding cyber safety among Nursing students: mixed method study" will be a bonafide and genuine research work carried out by me under the supervision of ***Dr.Prema.P*** *forpartial fulfilment*of the regulations for the Award of the degree of **Doctor of Philosophy** in **Nursing.**

Date: 28.4.2019

Signature of the Candidate

Ms. ANITHA .P

INTRODUCTION

"Our technological powers increase, but the side effects and potential hazards also escalate". --Alvin Toffler

The Internet is the major channel for education, creativity and self-expression, it is no longer only a framework and it has turned into a boundless space for data trade, informal communication, and the improvement of digital practices for human beings.[1]. As per a report distributed in 30th June 2014, the world's Internet client base was around 3 billion, in which approximately 1.4 billion clients are from Asia. The higher 45.7% is from Asian nations, Indians are the most noteworthy clients in Asia.[2]. In spite of the fact that individuals in all fragments of the general public utilize the Internet, particularly adolescents are the most continuous clients and in this manner progressively defenseless against Internet habit. [3]

Adolescence is a complex phase in that it is a bridging period between childhood and adulthood. Adolescents access the internet regularly and communication via the internet is especially popular among them.Adolescents are most commonly exposed to cybercrimes like cyber threats, cyber bullying, cyber grooming, email fraud, online transaction fraud, through online gaming and social networking profiles.[4]Cyber is a prefix derived from the word cybernetics and has the general meaning of through the use of a computer which is also called as cyberspace.[5] .The term 'cyberspace' is not novel, it has been used since the 1980's to refer to new technologies and devices which enable users to access the Internet and connect with others.[6].The cyber space connects millions of online users across the world and increasing use of cyber space parallelscybercrimes also increased. As per the NCRB survey report the reported cases of cybercrime was 5693 at

2013, at 2014 the reported cases was 9622, It increased 69.0% over previous year. As more people gain access to technology and the Internet, the need to teach users to navigate the online world responsibly and safety has become more urgent .[7]

Cyber safety or online safety or internet safety is to give knowledge and information about user's personal safety on internet and self-protection from computer crimes. The most recent NCRB (National Crime Record Bureau) distribution of 2017 demonstrates an expanding occurrence of cybercrime in India. Most extreme number of cases under digital crimes were accounted for in Uttar Pradesh (2,639) (21%) trailed by Maharashtra (2,380 cases) (19.3%) and Karnataka (1,101 cases) (8.9%) amid 2016. [8]. As an UNESCO worldwide youth overview of 2017 shows, 95% of the respondents trust that their online wellbeing is imperative to them, and 94% spot a high premium on the online security of others. Over 90% of those subjects feel that they should secure the fundamental abilities and capabilities to ensure themselves, rather than being checked by governments.[9]

Health care Professional students like nurses are also addicted for internet. A Descriptive Cross sectional survey study conducted at Metro College of Nursing Greater Noida, Uttar Pradesh, India. Its reveals among the students, 42% had mild, 34.02% had moderate, and 1.03% had severe internet addiction need to be educated about healthy use of internet.[10].Today, new models of learning have ascended to address the creating enthusiasm on skill building, paying little mind to age and insightful establishment by Online Courses.This is supported by quick advancement in information sharing through web and openness of specific devices to make the aptitudes of tomorrow. A study conducted on impact of online program on smoking in hospitals. It shows 202

participants out of which 99 of them completed pretest and posttest, result shows the increase in performance in various aspects they are Advise (7 to 9),Assess (6 to 8), Assist (2 to 7) and Arrange a follow up (0.52 to 5), Smoker and Doctors obtained a higher scores.[11] Likewise, online courses have ended up being more cost-effective, strengthen advising aptitudes that regularly can be hard to pass on in the conventional study hall setting, and permit separate realizing when nearby preparing chances and assets are rare.[12,13]

So the researcher feels that online course is the best method to convey message and there is a need to educate Nursing students about common cybercrimes, how to safe themselves to these problems .Since they are the healthcare professional, they can create awareness to others also regarding cyber safety. So researcher has chosen this topic.

REVIEW OF LITERATURE

Balhara YPS[1], Harshwardhan M[2], Kumar R[2], Singh S[3].(2018) conducted a prevalence study to assess the Extent and pattern of problematic internet use from cyber awareness program. 25 schools were participated in New Delhi, through random sampling method from middle, high, secondary and senior secondary grades 6291 students were selected and participated in study. The Generalized Problematic Internet Use Scale 2 was used and through self-report data was collected. Correlation analysis was done and a binary logistic regression was carried, result reveals that near about 19% of study participants faced problematic internet use. Problems are due to accessing social media, playing online gaming and fun for using internet. Researcher concludes that there is a need to educate all students about safe and healthy use of internet.[14]

Gudup Sarika Digamberrao (2018) conducted a survey study of Electronic Banking Frauds and Safety Awareness of Customers in Nanded District and provided information about safety E banking. Based on convenient sampling 400 adults are selected those who are above 20 years and ATM users for online transaction. Primary data was collected from the adult through structured questionnaire and secondary data was collected from bank reports, magazines, newspaper. Data were analyzed with mean percentage, standard deviation and chi square.112 (28%) of respondent don't feel online transaction is safe and secure and costumer were unaware about the safe E banking . Researcher collected the basic information from the bank managers about the safe use of E banking, in this researcher concludes that he also came to knew about the E banking and provided information to the customers and intervention programs to be taken for the online safety.[15]

Duc Tran1, Raghda Shukri1*, Diep Do2 (2018) conducted An analytical cross-sectional explorative study on Factors Related to Cyber Bullying among High School Students in Hanoi, Vietnam. Through a cluster sampling technique 406 students were selected from three grades of 10th, 11th and 12th at Chuong. Data was collected by using a standard questionnaire which was developed by Jing Wang in 2009. Result shows that 12.6 % of students were involved in cyber bullying, cyber victims were 10.2% and 4.2 % were both cyber bullies as well as cyber victims. Factors related to the cyber victims were students in violence, smoking history and history of family violence, $P < 0.05$.Researcher concludes cyberbullying is common and action to be taken to prevent the violence and awareness to be given to students.[16]

Vismara MF, Toaff J, Pulvirenti G, Settanni C, Colao E, Lavano SM, et al. (2017) conducted a study on Internet Use and Access, Behavior, Cyberbullying, and Grooming .The purpose of the study to assess the risks and risky behavior among adolescents and provide data to counsel the adolescents for the safe use of internet. It is a survey study in which 1534 students were selected in the city of Catanzaro, Italy. Through the structured closed ended questionnaire data were collected it contains 45 questions.Result reveals that 71.31% of the interviewed adolescents use their profiles on social networks of them knew all their Facebook contacts personally, 7.69% of the interviewed teenagers have uploaded pictures which they felt ashamed; 27.05% have received invitations from people they met online to meet personally and 8.67% had accepted such invitations too. The researcher concludes that through the research the risky behaviors are observed and guidance to be given at in their critical stage itself.[17]

Ibrahim a H. Çankaya a, Çetin Tan b (2010) conducted a study on Effect of cyber bullying on the distrust levels of preservice teachers and considered internet addiction as a mediating Variable . Through convenient sampling technique 380 samples selected they were preservice teachers and senior year students at the Firat University Education Faculty in Elaziig city. Cyber bullying scale, Internet addiction scale, Distrust scale were used data to collect data through self-report. Result shows that Cyber bullying of preservice teachers impacts directly their distrust levels at the 0.24 level. Internet addiction was included as a mediating variable and shows the direct impact of cyber bullying on distrust decreased to 0.14.It is reveals that cyber bullying is mediated by internet addiction, its impact on the distrust levels is more significant. Research concludes that possible measures to be taken to reduce the cyber bullying trough decreasing the exposure to cyber bullying.[18]

Aim

To develop online course on cyber safety for Nursing Students.

Objectives

1. To determine the effectiveness of online course regarding cyber safety among Nursing studentsin terms of change in knowledge.
2. To determine the level of perception and factors influencing online course regarding cyber safety as per viewed by Nursing studentsin experimental group.
3. To associate the pretest knowledge regarding cyber safety among Nursing students and with their demographic variables in experimental group.

Material and method

Research approach and design

Mixed method research approach,Explanatory Sequential mixed method is taking into account both quantitative and qualitative data.

Explanatory Sequential mixed method is Collection and analysis of both quantitative and qualitative data separately. Both data will be interpreted together to find out the depth comprehensive data.

Quantitative research: quasi experimental design,non-equivalent control group design.

Quantitative research is based on post positivism to know the cause and relationship, here in this study to know the effectiveness of online course on knowledge regarding cyber safety among nursing students through structured questionnaire. Here the researcher will be used quasi experimental method, non-equivalent control group design, in this pretest is observed in both the groups experimental and control. Experimental group receives treatment and later posttest will be observed in both groups.

Qualitative research: focus group discussion

Qualitative research is based on constructivism the exploration and provide comprehensive understanding of effectiveness of online course by perception and factors influencing online course which are experienced by experimental group through focus group discussion. Both the data are to be analyzed and interpreted in order to strengthen the study.

Study duration

The period of the study will be one year which will be used for the collection of data, evaluation and presentation of findings.

Population

Nursing students studying in school or college of Bareilly.

Sample and Sample size

Nursing students those have got enrolled and studying in GNM and B.Sc Nursing (1st year and 2nd year)in school or college of Nursing, Bareilly.

$$n = \frac{2(Z_{1-\alpha/2} + Z_{1-\beta})^2}{(d/\sigma)^2}$$

5% level of significance $Z_{1-\alpha/2}$ value is 1.96

90% power $Z_{1-\beta}$ value is 1.28

d/σ is effect size = 0.5 (acc. To cohen'd effect size)

Calculated sample size is 63.After including drop factor the researcher will be taking 70 samples for experimental group and 70 samples for control group

Qualitative research study

Focus groups will be formed and in each focus group is having 8 students. Focus group discussion will be focused on perception of online course regarding cyber safety and factors influencing online course. Focus group discussion will be conducted until a point of reaching the saturation. Saturation is when we get a same information repeatedly

Or the researcher don't get a new information it seems, received the end point of discussion.

Sampling technique

Quota sampling technique:

Quota sampling method is dividing the population into different quota and then selecting a sample without randomly from each quota. Here the population is nursing students divided into quota like GNM 1st year, GNM 2nd year, B.Sc. (Nursing) 1st yearand B.Sc. (Nursing) 2nd year. Proportionately from each quota samples will be collected without randomly.

Inclusion criteria

- ✓ Nursing students who are available and willing to participate in study
- ✓ Age group of 17 to 19 years
- ✓ GNM and B.Sc. Nursing 1st year and 2nd year students.

Exclusion criteria

- Nursing students who are not willing to participate.

Development of tool

Tool 1: Demographic tool

Tool 2: Structured questionnaire to find out the knowledge on cyber safety

Tool 3: Focus group discussion will be related to the perception on online course regarding cyber safety and its influencing factors.

Description of tool

Tool 1: Demographic variable such as place of residency, number of siblings, mode of internet access, total hours of time spending in online, mode of social media, type of mobile.

Tool 2: Structured questionnaire contains the knowledge on cyber safety in seven aspects, they are cyber bullying, cyber grooming, identity theft, plagiarism, online gaming, email fraud and general online transaction fraud.

Tool 3: Focus group discussionwill be focusing online course on certain aspects like standard program content, focuses on adolescent, interactive and difficulties.

Interpretation of tool

Tool 2:

Component	**Scores**
cyber bullying	5
cyber grooming	5
identity theft	5
Plagiarism	5
online gaming	5
email fraud	5
General online transaction fraud.	5
Total score	**35**

Poor = 0-11

Average = 12-23

Good= 24-35

Tool 3: according to coding and theme analysis.

Data collection procedure

Permission will be obtained from the administrator of selected college of nursing and informed consent will be taken from the nursing students. Structured questionnaire will be administered to the experimental and control groups to check the pre knowledge level regarding cyber safety.Online course regarding cyber safety will be administered to the experimental group. Following this after seven days posttest knowledge will be assessed through questionnaire for both groups. Nursing students are selected from experimental group for focus group discussion regarding perception regarding online course and factor influencing online course.

Data analysis

Quantitative data

Descriptive and inferential statistics are used to analyses the data

Descriptive statistics

Mean, percentage and standard deviation are used to analyze the knowledge level of Cyber safety.

Inferential statistics

Chi square test is used to find out the significant association with the demographic Variables. Paired and unpaired T-test, ANOVA will be used to analyze the effectiveness of online.

Qualitative data

All of the information obtained from the focus groups will be documented and analyzed. The collected raw data will be texted into word processing document. Then the developed data will be organized into different concepts in such a way to identity relevant pattern. The coded segments will be grouped and synthesized into categories which in turn get linked to more general themes. Thematic analysis will be done to summarize all the concepts. Some software packages like ATLAS,NVIVO and MAXQDA will be used to analyze the qualitative data.

REFERENCE

1. Mak K-K, Lai C-M, Watanabe H, Kim D-I, Bahar N . Epidemiology of internet behaviors and addiction among adolescents in six Asian countries. Cyber psychology, behavior and social networking. United States.2014; 17: 720-728.

2. Choi K, Son H, Park M, Han J, Kim K. Prevalence and correlates of excessive internet use among youth in Singapore. Ann Acad Med .2008; 37: 9-14.

3. Ha HJ, Kim YS, Bae SC, Kim H, Sim M. Depression and Internet Addiction in Adolescents. Psychopathology.2007; 40: 424-430.

4. Ministry of home affairs .hand book for adolescents /students on cyber safety . 2018 oct 31. Available from: https://mha.gov.in/sites/default/files/CyberSafety_English_Web_03122018.pdf

5. The department of science and technology. Basic research of science and technology. 2017 Jan 9.Available from: http:dst.gov.in/basic-research-cyber-security.

6. Ministry of home affairs .hand book for adolescents /students on cyber safety . 2018 oct31. Available from:https://mha.gov.in/sites/default/files/CyberSafety_English_Web_03122018.pdf

7. Blashill, Aaron J.; Wilhelm, Sabine .Body Image Distortions, Weight, and Depression in Adolescent Boys: Longitudinal Trajectories into Adulthood. Psychology of Men & Masculinity.2014; 15(4):445-451.

8. Crime in India. National crime records Bureau.2017 Oct 10.Available from: http://ncrb.gov.in/StatPublications/CII/CII2016/pdfs/NEWPDFs/Crime%20in%20India%20-%202016%20Complete%20PDF%20291117.pdf.

9. Yasmin Ali Haque and Eric Fait. Why India should make online child safety a priority. Hindustan times. 2019 Feb 11.

10. Jithin Thomas Parel[1], Linsu Thomas[2] .Level of Internet Addiction among Nursing Students: A Cross Sectional Survey. Asian J. Nur. Edu. and Research.2017; 7(4): 466-470.

11. Martínez, C., Castellano, Y., Company, A., Guillen, O., Margalef, M., Alicia Arrien, M. study project, T. G. O. H. C. I. T. F. (2018). Impact of an online training program in hospital workers' smoking cessation interventions in Bolivia, Guatemala and Paraguay. Tobacco Prevention & Cessation, 4(Supplement), A146.

12. R. Aggarwal, N. Gupte, N. Kass, *et al.* A comparison of online versus on-site training in health research methodology: a randomized study .BMC Med Educ: 11 (2011); p. 37.

13. S.M. Abutarbush, J.M. Naylor, G. Parchoma, *et al.* Evaluation of traditional instruction versus a self-learning computer module in teaching veterinary students how to pass a nasogastric tube in the horse J Vet Med Educ., 33 (2006), pp. 447-454.

14. Balhara YPS[1], Harshwardhan M[2], Kumar R[2], Singh S[3]. Extent and pattern of problematic internet use among school students from Delhi: Findings from the cyber awareness program. Asian J Psychiatric. 2018; 34:38-42.

15. Gudup Sarika Digamberrao. Electronic Banking Frauds and Safety Awareness of Customers .Shodhganga. Available from: http://shodhganga.inflibnet.ac.in/handle/10603/230016.

16. Tran D, Shukri R, Do D. Factors Related to Cyber Bullying among High School Students in Hanoi, Vietnam. Canad J Clin Nutr 2018; 6 (1): 107-122.

17. Vismara MF, Toaff J, Pulvirenti G, Settanni C, Colao E, Lavano SM, et al. Internet use and access, behavior, cyberbullying, and grooming: results of an investigative whole city survey of adolescents. Interactive journal of medical research. 2017 Jul; 6(2).

18. İbrahim H. Çankaya, Çetin Tan. Effect of cyber bullying on the distrust levels of preservice teachers. Procedia - Social and Behavioral Sciences; 2010 (9):1634-1640.

ANNEXURE – B

LETTER SEEKING EXPERT'S OPINION AND SUGGESTION FOR THE CONTENT VALIDATY OF THE TOOL

From,

_____

_____

_____

_____

To,

_____

_____

Respected Sir/Madam

Subject:- Request for expert opinion and suggestion to establish content validity of the research tool.

I_____ Phd scholar, Faculty of Nursing have undertaken a research project work on

_____

_____

_____

_____Which to be submitted to Bareilly International University, Bareilly for Partial fulfillment of Phd in Nursing.

I humbly request you to go through the content and give your valuable suggestions and opinion.

Thanking you

Yours Obediently

_____

ANNEXURE – C

CRITERIA PRACTICE SCALE FOR EVALUATION OF TOOL

Dear Sir/Madam

Kindly go through the tool content; give opinion in the columns given in the criteria table against to each question. If the item is not relevant, please give your valuable suggestion in the column.

I team No:	Not Relevant	Relevant to some extent	Relevant	Remark
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				

SECTION B:- Knowledge Questionnaire

I team No:	Not Relevant	Relevant to some extent	Relevant	Remark
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
19				
20				
21				
22				
23				
24				
25				
26				
27				
28				
29				
30				
31				
32				
33				
34				
35				

General Comments_____

_____

Date: **Signature of Experts**

Place: **Name of Designation**

LETTER REQUESTING PERMISSION TO CONDUCT MAINRESEARCH STUDY:-

From,

_____

_____

_____

To,

_____

_____

Subject:-Requesting permission to conduct main study.

Respected Sir/Madam

I_____ Phd scholar, Faculty of Nursing have undertaken a research project work on

_____

_____

_____

_____Which to be submitted to Bareilly International University, Bareilly for Partial fulfillment of Phd in Nursing.

This study is approved by the ethical committee of Bareilly international university. Regarding this main study, I am is in need of your esteemed help and co-operation as i am is interested in conducting a study in ----------

I request you to kindly permit me to conduct the proposed study and provide me the necessary facilities. I will furnish future details of the study, if required personally. Please do the needful. I assure that this study will not make any harmful effects on the subjects.

Thanking you in anticipation

Date:
Place:

Yours Faithfully

PRINCIPAL

Module
On
Cyber safety

Introduction

Cyber is a prefix derived from the word cybernetics and has the general meaning of through the use of a computer which is also called as cyberspace.The cyber space connects millions of online users across the world and increasing use of cyber space, cybercrimes also increased.

Cyber safety or online safety or internet safety is to give knowledge and information about user's personal safety on internet and self-protection from computer crimes. Adolescents are most commonly exposed cybercrimes so this course is created for adolescents to give awareness about various cybercrimes like cyber bullying, cyber grooming, identity theft, plagiarism, online gaming, email fraud and online transaction fraud.

Objectives

At the end of the course the students will be able to,

1. Get awareness about various cyber crimes
2. Understand online behaviors
3. Understand the impact of various cyber crimes
4. Discuss about how to prevent cybercrimes and steps to taken to tackle it.

CYBER BULLYING

Cyber Bullying is the use of the Internet and related technologies to harm other people in a deliberate, repeated, and hostile manner.

SevereformsCyber Bullying

- Cyber Bullying is taking place in various forms like posting, public photos, Sending inappropriate text messages, giving negative comments, Blackmailing with certain demands, Threats of violence or death, aggressive communications or actions, posting recorded photos or videos which are taken without the subject's knowledge, Sexually explicit.

Cyberbully occurs through:

- personal websites
- blogs
- e-mail
- texting
- social networking sites
- chat rooms
- message boards
- instant messaging
- photographs

Effectsof cyber bullying

- ❖ Those who are cyberbullied are also likely to be bullied offline
- ❖ Undermining confident
- ❖ Stress and hurtful health effects
- ❖ Lower performance and attending level at school

- ❖ Depression and a way of loneliness
- ❖ Suicidal thoughts

Preventionof cyber bullying

- ✓ Tell to trusted person
- ✓ Ignore it
- ✓ Block them
- ✓ Always log out
- ✓ Attempt to identify the cause.
- ✓ Save the evidence.
- ✓ Report the person to service providers.
- ✓ don't be cyber bully yourself

How to Prevent It

- **Never**- share your passwords, private photos, or personal data online, not even with friends. Try to limit your identity.
- **Privacy settings**- on social media to select those who can access your posts online. Restrict access of your profile only to your friends.
- **Think**-before you post. When you're sad, angry or depressed wait to post or respond.
- **Never**- publicly post anything whichwouldn't be comfortable with people who knowing you like your parents and friends.
- **Never** install unwanted Software and Apps like dating apps, online games, etc. from unknown sources.

Want to do if you're being cyberbullied

- ***Tell*** your parents or another trusted adult.
- ***Don't respond***—they might use it against you
- ***Block*** the bully and change your privacy settings
- ***Save everything*** – emails, messages, posts, screenshots etc.save the proofs don't delete it.
- ***Report-to*** Social media sites where you have ways of reporting harassing content with proofs.

If you are one of the observer

If you see someone being bullied online:

- ***Don't participate***. Don't entertain, don't "like" or share any post that are bullying someone.
- **Report it**. Still you can report it though the content is not targeting you

CYBER GROOMING

The cyber groomers can utilize gaming sites, online networking, email, talk rooms, texting, and so on by making a phony record and professing to be a youngster or having same interests as of the youngster.

The greater part of them don't understand that somebody is preparing them on the web. Groomer can be a known individual or an obscure.

In the first place the cyber groomer can get a sure through giving you compliments, blessings, work offer and later they can begin sending revolting messages, photos or recordings and will request that you share your explicitly express pictures or recordings with them.

The cyber preparing has profound effect on a youngster's physical, passionate just as mental prosperity. It can affect their scholastic execution as well as their day by day life all things considered. The overwhelming impacts of web based preparing can here and there be long haul and can even frequent the injured individual in their adulthood

Signs of grooming

Online groomers are really good in the beginning. Which means it can be difficult to get if someone is really an online friend, or if they're trying to get you to send them sexual images or videos.

Some of the following they can do:

- Send you lots of messages
- Ask you to keep your conversations secret
- Try to find out more regarding your privacy
- Start sending you sexual messages
- Get to know about your personal information for try to meet you
- Blackmail you

How you can protect yourself from cyber grooming

Never give out your real name

- Don't accept friend request from unknown people on social media.
- Don't share your personal information like date of birth, address, phone number and school name on social media or other online platforms. You can go to privacy

settings on social media platforms to select who can access your posts online. Try to restrict access of your profile to your friends only.

- Be cautious when your chat partner gives you many compliments regarding your appearance in just a short span of your contact.
- Avoid talking to people who asks you questions about physical or sexual experiences. You can warn the person to stop asking you such type of questions and immediately inform your parents
- Do not talk to people who ask you to share your sexually explicit photographs or videos. If you share your photos, the person can share to others and also blackmail you.
- Informto your elders or parents, if the person wants to maintain a secret conversation with you.
- Do not try to meet a person to whom you met online alone.
- Never install unwanted Software and Apps like dating App, online games, etc. from unknown sources

What can you do if you are a victim of cyber grooming?

- Inform your parents / elders immediately:
- Block the Groomer
- Collect and Save messages.
- Your parents/elders can contact local police station to lodge a complaint against the groomer.

IDENTITY THEFT

Identity theft is in which someone steals others personal information to commit fraud like getting false credential, opening new accounts etc.

Types of ID Theft

- Social ID theft - Someone uses your personal information like name and photos to create a fake account on social media

- Tax ID theft - Someone uses your Social Security number to falsely file tax returns with the IRS or your state
- Medical ID theft - Someone steals your Medicare ID or health insurance member number to get the medical services.

How it happens

Hackers can get your personal information on social media or offline. these informations include :

- full name, address and date of birth
- bank account number or credit card number
- medical insurance number or other insurance numbers
- details related with account recovery question details
- social security numbers

There are some following ways the thieves can steal your informations offline

Shoulder surfing

Thieves can steal your informations on your shoulders when you're typing sensitive informations on computer, ATM or phone or while you're on call and giving informations.

Dumpster diving

Thievescan get your informations through discarded checks credit card and valuable personal informations in garbage.

There are some following ways the thieves can steal your informations online

Unencrypted websites –you have tomake it sure for your website whetherit is safe or not before transaction .you to check for the lock picture in the URL field ,URL contain "https" here the last letter "s" means the website it is secure and "https" in a small letter not in capital.

Public Wi-Fi – public Wi-Fi for the most part doesn't encrypt data, so anybody with the Wi-Fi secret word and some programmer know-in what manner can screen what you see and what you send. The programmer could submit fraud on the off chance that the individual captures your information.

Phishing- Watch out foridentity thieves who get in touch with you from a telephone number or email address custom fitted to look well-known and dependable. The objective is to get individual data from you.

What to search for? A fishy email may have wrong spelling or sentence structure, an informal looking email address, which is in urgent base looking for information and have an attachments or links.

In the event that you get a suspicious email, contact the substance yourself and confirm it's extremely an email from the individual or organization you trust.

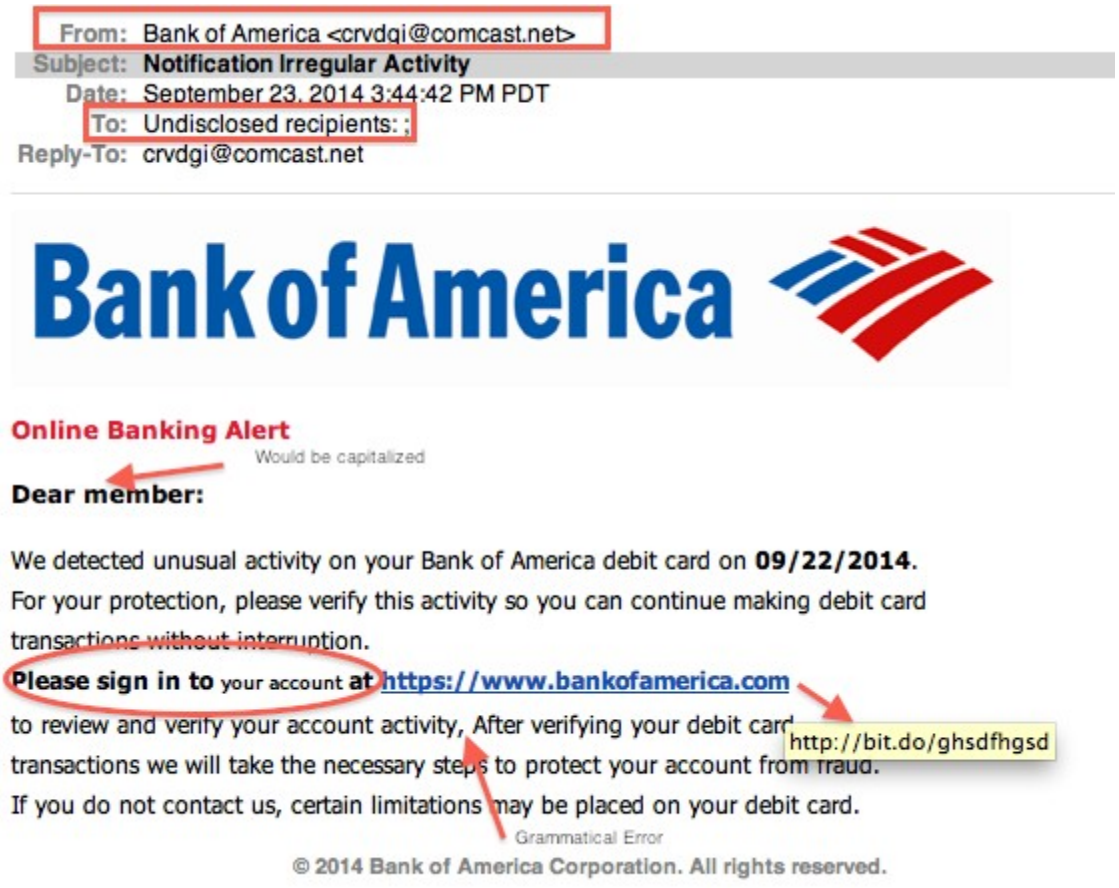
Phishing

Phishing is the act of sending email to a user to attempt to get sensitive information like password, credit card bank accounts number by acting like a trustworthy entity.

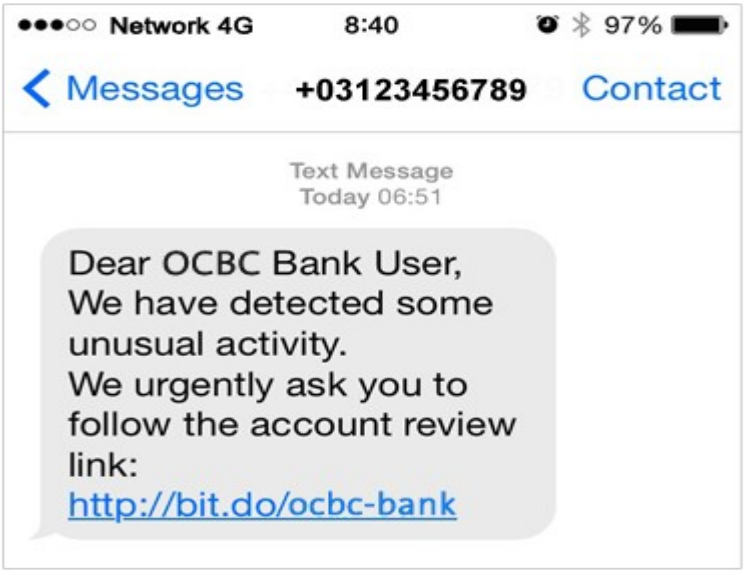
These emails pretend to be from banks or government departments and it has the fake websites. Sometimes these emails don't have the links or documents but once you open these attachments, without your knowledge it installs malware in your computer.

How to find out the phishing email.

- the sender address will be misspelled and unusual address
- it use generic greetings since that mail sent to hundreds of people
- it has grammar and spelling mistakes
- It always makes a sense of urgency.it encourage you to download a file or clink a link to avoid a problem.
- It has a malicious attachments. When you open the documents it runs automatically to infect your computer.


From: Bank of America <crvdgi@comcast.net>
Subject: Notification Irregular Activity
Date: September 23, 2014 3:44:42 PM PDT
To: Undisclosed recipients: ;
Reply-To: crvdgi@comcast.net
Bank of America
Online Banking Alert
Would be capitalized
Dear member:
We detected unusual activity on your Bank of America debit card on 09/22/2014.
For your protection, please verify this activity so you can continue making debit card transactions without interruption.
Please sign in to your account at https://www.bankofamerica.com
to review and verify your account activity, After verifying your debit card
http://bit.do/ghsdfhgsd
transactions we will take the necessary steps to protect your account from fraud.
If you do not contact us, certain limitations may be placed on your debit card.
Grammatical Error
© 2014 Bank of America Corporation. All rights reserved.

examples of SMS phishing



What to do for phishing message

- ❖ Don’t response even it has the sense of urgency
- ❖ Don’t fill the information that email asks you to give.
- ❖ Review your personal information like credit card and bank statement, address, phone number is correct.
- ❖ Make it sure for you’re on the right website.
- ❖ If you receive a phishing email or text message can report it immediately to incident@cert-in.org.in

Warning signs of identity theft

You see withdrawals from your financial balance that you didn't make.

• You don't get bills or other mail.

• You get calls from obligation authorities on debts you didn't bring about.

• You see new records or charges on your credit report.

•You get hospital expenses for administrations you didn't get.

• A health plan won't guarantee you because that your therapeutic records demonstrate a condition you don't have.

• The IRS sends you a letter saying more than one expense form was documented in your name. Or on the other hand the IRS informs you that you have pay from a business you never worked for.

Prevent identity theft

- Secure your Social Security number. Don't leave it on public place.
- Never share your personal information like birthdate, Social Security number, or bank account number if someone asks for it.
- Pay attention to your bills
- Use the security features on your mobile phone.
- Use always a secure Wi-Fi.
- Check for your credit card and bank account statements.
- Never leave your personal information to prevent "dumpster divers".
- Store personal information in a safe place.
- Create complex passwords so that identity thieves cannot guess.
- Following these steps will help you easily create a strong password:
- Use more than one password.
- Using the same password for multiple accounts is an easy way to lose everything you have. Use different passwords so that if one account is broken into, the others will stay safe.
- Be Relevant.
- Make a password that you will recognize, but to others it seems random. Never use information that can be directly related to you in your password; like your name, social security number, address, etc.
- Use (not-so) random characters.
- A password that looks random to the naked eye and it should be perfect. For example: MFFIM98 seems like a bunch of gibberish but is easily translated into:

My Favorite fruit is mango and the numbers could refer to anything, like your birth year.

- Length is important - The longer your password is, the harder to figure out what it is. This is the reason for a minimum character length on most websites that you have accounts on.
- Use the SUPR test.

  S - Strong (should have random numbers and letters)

  U – Unique (not related to other password)

  P - Practical (can recall without writing it down)

  R - Recent (whether you changed recently)

ONLINE GAMING

Gaming is another area which has been changed with the coming of data innovation. An ever increasing number of children are joining the internet gaming network. Children can play web based recreations on mobiles, PCs, compact gaming gadgets and social networks. You not just play amusements with crores of clients on the web yet additionally converse with them, share your perspectives, become companions, join gatherings, groups, and so forth. While web based amusements can be fun which additionally bring related dangers.

Risks of online games

1. Many aggressive online players who may bully you. Some of them play intentionally to bully others.

2. Many cybercriminals pretend like they are children and try be friend with others. After gaining confident with others try to get personal information for grooming.
3. There are many free internet gaming sites. Additionally you may get links and emails to download and get personal information like your name, age, mobile number, and so on, which can be abused. You may finish up downloading infections or malwares which may infect your computers
4. In numerous internet games you're requested to purchase points /coins, and so forth. and. You are approached to share credit card details for the payments. Moreover some infected online games can save your credit card details and do cybercrimes.

How you can protect yourself while online gaming

- Link based scams and phishing is common in game chat so when you are receiving from the stranger we have careful and don't open it.
- Never share your account information if you get an email and says you won the prize ad asked you to enter the user name and password. Always use two factor authentication to protect your account.
- Don't use personally identifiable information. Never use this because its leads to identity theft.

Personally identifiable information

- Full name
- Postal address

- Name and address of school
- mailing address and phone number
- Passwords
- Credit card number
- Social security number
- work place
- Photo's

These are the examples you can share

- age
- sex
- number of siblings
- favorite color
- favorite food
- The name of your pet
- Your opinion about some common issues

- Make a habit of change your password regularly.
- Never download games by the links which you have received by mail or text message or through a popup. You may wind up downloading infections and malwares which can bargain security of your PC or mobile.
- Never meet face to face with somebody from your online gaming world.

- If you face any problem in internet gaming world, quickly inform to your parents or to adult to whom you trust.
- Create a habit of playing outside recreations. You will appreciate open air exercises and can make genuine great companions

PLAGIARISM

"Plagiarism is the wrongful appropriation and purloining and publication of another author's language, thoughts, ideas, or expressions, and the representation of them as one's own original work."

What is Plagiarizing?

- Neglecting to put a citation in quotes.
- Giving mistaken data about the source of a citation.
- Asserting another person's work as your own.
- Changing words yet duplicating the sentence structure of a source without giving credit.
- Copingwords or thoughts from another person without giving credit.
- Having most of your work originated from a particular source, regardless of whether you give credit or not.
- Losing a reference in your work.

Effects of plagiarizing

Plagiarizing is a serious situation so in order to avoid it before we get into safely using copyrighted works, let’s see the consequences whatmight happen if you directly copy another's work.

Expulsion

From school tocollege gives the punishment for plagiarism like expulsion

Court

Stealing someone else's work is called copyright infringement. According to that some time it may end to stand in front of a judge and jury.

Fines

Penaltieswill be applied for the act of infringement

What is mean by copyrighted?

The copyright law covers the following categories:

Abstract works

Both fiction and verifiable, including books, periodicals, original copies, PC programs, manuals, phono records, film, audiotapes, and PC plates.

Melodic works

Going with words, melodies, musical dramas, and melodic plays.

Sensational works

Counting music, plays, and sensational readings

Choreographed works

Like dance or schedules in shows.

Pictorial, illustrations, and sculptural works

Last and connected expressions, photos, prints, maps, globes, outlines, specialized illustrations, graphs, and models.

Films and varying media works

Slide/tape, sight and sound introductions, filmstrips, movies, and recordings.

Sound Recordings

Tapes and PC disks.

Fair use

Fair use is some sources that you can copy withoutgiving to cite. This method of copyrighting is called fair use. There are some areas which we are mentioned below:

- Works that not having originalitylike phone books.
- Public domain works can be used by anyone.
- The work is claimed by the Government.
- Any work distributed prior to December 31, 1922
- Freeware - Software found online that the creator has made accessible to anybody with no confinements

Using copyrighted works safely

- Cite all of your sources and quotations when you used some ones work and then include a works cited at the end of your work.
- Citation includes the author's name, year of publication, publisher name, thedate, and so on.
- Do paraphrasing – don’t do quotation marks but cite the other works.

- There are various plagiarism detector tools to check the plagiarism like paperrator,plagiarism,plag tracker etc. Plagiarism detector highlights the material that exactly matches to the original author's words if you are not paraphrased.

EMAIL FRAUD

The greater part of you have your own email account. We need an email account not simply to send messages to our loved ones yet in addition for opening a web-based social networking account, web based gaming account and other online records. Our email account has turned into an indispensable piece of our life. As you will grow up, utility of your email record will increment. You will utilize your email represent interfacing with bank, portable specialist organization, speak with your school, and so on. It is essential to figure out how to protect your email account.

Email fraud is normal and most economical technique utilized by cyber criminals to bargain other email represents individual increase or to make harm person.

How it happens

There are many ways a cybercriminal can use an email to trigger an attack on your system or collect your important personal information.

A cybercriminal settling down anyplace in the world can send you an email which may like from a fake account. you may get to know the fake account by seeing the mail for example spelling might be slightly changed - customer support @ gamingpportal.com here you can see the pportalspelling is wrong. These messages contain joins which would guide you to another page where you would be approached to enter

passwords/certification for upgrade. Lastly you end up giving your accreditations to cybercriminal.

- Another way generally utilized by cybercriminal is sending an email with an attached file (word or excel file) which may contain malware (hazardous program that can affect your PC).Thetitle shows that tips to win the game or to get free the coins. If you install such documents it may catch your id and password from your computer and send them to others.

- Do such messages they ask for the personal informations like bank details for sending the amount or they may ask the processing fee to send the gift or amount. Such emails are fake so better to not respond to such mails.
- Emailhacking is one of the way the cyber criminals follows to get you mail id and password through malware. Once its hacked it may direct them to other social media accounts, bank accounts etc. Moreover they send mail to others those who are in your address book and seek for financial help or for cyber grooming.

How you can protect yourself

- Before opening the email first for the sender name
- don’t reply to SPAM
- change your password periodically
- Create a strong and complex password so that criminals unable to hack your email. Password always should be difficult to guess so which has combination of words and numbers

- Alwaysuse two factor authentication for login. It is always allow you to login through password and OTP which you receive into your registered mobile number.it will help you to keep your account safe.
- Never share password of your email account with anyone.
- Don't click online or attachment which you have received from unknown sender.
- If you use others computer for email access make it sure that to sign off after the use and never click the option of “remember password popup" .change the password once you used the public computer.
- If your email is hacked immediately block your email id through your service provider by help page. Take action to change your password.
- Never install unwanted software and apps from unknown sources. Never click on links or files received from unknown person on your email or over message. This may be an attempt to infect your computer/ phone with malware.
- If you receive an email about winning a lottery orprize, please don't respond to it and share your personal information like name, address, bank account details, etc.
- develop a habit of changing the passwords at regular intervals
- Don’t reply to the strangers
- Inform to parents in case of mail message make you to feel uncomfortable.

ONLINE TRANSACTION FRAUD

Online transaction fraud means withdrawing or transferring money illegally by a cybercriminal from your account to another account. Online transaction frauds can happen by a criminal when they steal your bank account details or credit card details.

How it works?

There are certain following ways used by cyber criminals for online transaction fraud.

Cyber criminals pretend you like they are bank or credit card services provider and send you the email. Once you open the mail and clink the link, you will be asked for the bank account details, card details, card verification value (CVV), expiry date, etc., after sharing these details, your account can be compromised.

Cyber criminals may make a fake call posing as a bank employee and try to obtain credit card or bank details such as account number, personal identification number (PIN), CVV, expiry date, date of birth, etc. after getting these details, the account can be compromised.

Cyber criminals may call you, pretendingas an employee of mobile service, provider and inform you to update your SIM(Subscriber Identification Module) otherwise your mobile number will be disconnected. They will send you a link to update the SIM and ask you to send a SMS to block the current SIM and issue a duplicate SIM. After getting a duplicate SIM they use for online transaction and banking app.

How you can protect yourself from online transaction frauds

- Never share your bank and card details such as online account. Password, card number, CVV, expiry date, PIN, OTP, etc., with anyone.
- Make it a habit to regularly update your bank account transaction details and PIN of your Debit/Credit Cards.
- Never ask someone to login your account operate by yourself.
- Try to findout the fake websites.
- Check for the bank's security certificate details and various signs such as green address line, lock sign on the address bar and https to confirm you are visiting a secure bank website.

- It’s very necessary to keep your mobile phones safe as your number is linked with your bank account. Usestrong password to open your phone.
- Always install a good antivirus on your computer and mobile phone.
- Avoid making online transactions by using a public Wi-Fi or in a cyber café. Computers which are in the cyber café may not have updated antivirus so it may compromise your bank details.
- Make it a habit to review the monthly statements of your bank account and credit cards. Check if there is any unrecognized transaction.
- In case of unrecognized transaction immediately report to your bank.
- If your debit card/credit card is got missed immediately block your card.
- there are some techniques to create a password they are,
    - create a strong passwords .minimum of 10 characters includes
        - lower case and upper case letters
        - numbers
        - special characters like @, + and *
    - Use passphrase – it is a collection of words which gives you the meaning.eg myfavouritecolorisblue.
    - Password should be hard to guess-avoid personal information like date of birth, your children name etc.
    - Try to avoid dictionary words, keyboard pattern like zxcvb
    - repeated characters like bbbb
    - Use different password for each account, don’t keep the same for easy remembrance.

- Keep your password in safe place. Never write it down. There are some app like password safe just you have to save all passwords in that app and need to remember the app's password.

- Clear your history, cache and cookies in your browser security.it is better to clear all these information especially when you are using the public computer.
- Check for the secure site. Always check the website URL starts with https. The website URL with https encrypts your data in the website and protects it from any kind of tampering. Do not share your confidential information such as online account password, card number, CVV, expiry date, PIN, OTP, etc. on the website which doesn't start with https. Check for the green lock and spelling mistakes.

KNOWLEDGE QUESTIONNAIRES

Cyber Bullying:

1.Cyber is define as:

a) Communicate each other face to face

b) Use non-verbal technique to communicate

c)Culture of computer information technology and virtual reality

2.Bullying is:

a) Seek to harm

b) Seek to care

c) Seek to reassure

3.Cyber Bullying is define as:

a) Punching a person in the face

b) Saying "I hate you" to a friend

c)When a person is being harassed over the internet

4.Protect yourself from cyber bullying by:

a) Don't share your personal information

b)Talking about your personal life

c) Giving details about your family members

5.If anyone harm you by posting any vulgar comment/videos, you should:

a) React with aggressive replies

b) Inform your parents and elders immediately

c)Replywith embarrassing pictures/videos

Cyber Grooming-

6.Cyber grooming is defined as:

a)Process of befriending a young person online to facilitate online sexual contact and/or physical meeting with the goal of committing sexual abuse

b)Process of befriending a young person face to face sexual contact

c)Online chat

7. The groomer interacts with you through:

a)Letters

b)Using gaming websites, social media, e-mail, chat room

c)Face to face meeting

8. Groomer can attract you by:

a)Giving you compliments, gifts, modelling job offers

b) Sending abusive posts

c)Awful chats

9.When online friends say they want to meet you in person, you should:

a) Go ahead, make plans and meet them wherever and whenever they want

b) Inform your parents and make sure that you meet there are a lot of people around

c) Never meet anyone in person that you met online, it's just not safe

10.You save yourself from cyber grooming

a) Meeting to the cyber friends

b)Avoid talking people who questions you related to your physical and sexual experience

c)Perception is given by cyber groomer is always right

Identity Theft:

11.Identity theft is known as:

a) Identity fraud(someone steals others personal information to commit fraud)

b) Identity friend(your online friend)

c) Identity relatives

12.Example of secure internet site is

a) http://customerservice.com

b) **https://customerservice.com**

c) Http://customersercice.com

13.When you are making up a user name for email and instant messaging, you should:

a) Always use your real name

b) Use a name that does not reveal your true identity

c) Use a name that gives good clues about who you really are.

14.How do you keep your profile safe on Facebook:

a) I show everyone my password

b) I let everyone see my pictures, post etc.

c)You have to keep your account safe on Facebook, by changing all the privacy settings to private so that ONLY your friends can see the posts on your wall and pictures etc.

15.How can you prevent from becoming a victim of identity theft? Choose the best possible answer:

a) Share your personal information to ads or websites that say you won an iPad, vacation, or other prize

b) Shop from sketchy websites you do not trust

c) Do not respond to ads or websites that say you won an iPad, vacation, or other prize

Plagiarism:

16.Plagiarism is:

a) Use to describe malicious software like malware

b) Type of cyber terrorism

c) Access to copyrighted material without license is illegal itself

17. Consequences of plagiarism:

a) You might end up in front of judge and jury

b) No any punishment

c) Can continue as they are copyrighting

18. How to reduce plagiarism:

a) By sharing the links of copied material

b) Initiate student to copy others work

c) By appropriate student assessment, draw on personal experiences and promote students to do their own work

19. Benefits of plagiarism detector is:

a) Gives correction to the content

b)You can compare with original documents for similarities

c) Cannot compare the documents

20. Copyright law covers

a) Literacy works, music works, plays, dances, pictures, graphs, A.V. works

b)Only literacy works

c)Pictures and graphs

Online Gaming:

21.Risk associated with online gaming:

a) Many cyber criminals also play online games to bully or harass others

b)Enjoy online games and entertain yourself

c) Best platform to make friends

22. If anyone asked about your credit/debit card details for move into next level in game then:

a) Share your bank account details

b)Never share your bank account details

c)Ask them their bank account details

23. Being a victim of online gaming will be saved by:

a)Share details of your phone

b)Share details of IP address

c)Never share your password of your phone, computer, voice chat and web cam

24. If online games ask you to buy points/coins, you should

a) Ignore them

b) Buy points /coins by giving bank account details

c) Respond them immediately

25. Play online gaming safely by:

a)Accepting all online games requests

b)Follow safeguards to protect yourself from potential risks associated with online gaming

c)Sharing personal details

<u>E-mail Fraud-</u>

26.Password of your e-mail id:

a)Should be long, strong, unique and not to be easily guessed

b)Should be easy to guess

c)Password should be same for different accounts

27. Ways used by cyber criminals to hack an e-mail through:

a)Sending large GB documents

b)Malware (dangerous program that can impact your computer)

c) Online video calls

28. Safeguard your email by

a)Use same password for a longer period

b)Always use one factor authentication

c) Using "remember password popup"

29.When you get an email or instant message from people you don't know, you should:

a)Ignore it and put it in your trash folder

b) Respond with a polite how do you do

c) Forward the message to your best friends

30. You see one of your friends typing in their password to a social networking site, what do you do?

a)You tell your friend that you have seen what her password it and you ask her to change it just in case anyone else saw her typing

b)Go on and tell every one of her friends that she is a total loser

c)Tell the password to all of your mates, so that they can all go on to the page and tease her on it.

General Online Transaction Frauds:

31.Online transaction fraud means:

a)Deposit money to account through bank

b)Taking cash money from your home

c)Illegally withdrawing or transferring money from your account to another account by cyber criminals

32. Check bank security certificate for

a)Red address line

b)Lock sign on the address bar

c)Website URL starts with http

33. Cyber criminals can hack your account by:

a)Enclosing your account number, PIN,CVV and expiry date

b)Asking name and address

c)Asking family member's name

34. If your debit/credit card is lost or stolen:

a)No matters and get the another card

b)Complaint to bank helpline number and block your card immediately

c)Give your bank details to someone

35. If you are using mobile app banking then:

a)Use official bank app

b)Use any bank app

c)Use the unofficial websites

DEMOGRAPHIC TOOL

1. Place of residency

(a) Hosteller

(b) Day scholar

2.Number of sibling

(a) 0-1

(b) 2-3

(c) 4-5

(d) Above 5

3. Mode of internet access

(a) Mobile

(b) Broad band

(c) Wi-Fi

4. Total hours of time spending in online

(a) Less than 1 hour

(b) 1-2 hours

(c) 2-3 hours

(d) More than 3 hours

5. Mode of social media

(a) Facebook

(b) WhatsApp

(c) Messenger

(d) Others

6. Type of mobile

(a) Tablet

(b) Apple

(c) Multi media

(d) Android

(e) Microsoft’s types of phone

CONSENT FORM

Title of the Research:

Participant's name: Address:

The purpose of the study have been provided to me in writing and explained to me in my own language. I confirm that I have understood the above study and had the opportunity to ask questions. I understand that my participation in the study is voluntary and that I am free to withdraw at any time, without giving any reason. I agree not to restrict the use of any data or results that arise from this study provided such a use is only for scientific purpose(s). I fully consent to participate in the above study.

Signature of the participant: _____ Date: _____

Signature of the investigator: _____ Date: _____

CONSENT FORM (for participants less than18 years of age)

Parent/Legally acceptable representative (LAR)

Title of the Research:

Participant's name: Address:

Parent/LAR' s name:

The purpose of the study have been provided to me in writing and explained to me in my own language. I confirm that I have understood the above study and had the opportunity to ask questions. I understand that my child/ward's participation in the study is voluntary and that I am free to withdraw my child/ward at any time, without giving any reason. I agree not to restrict the use of any data or results that arise from this study provided such a use is only for scientific purpose(s). I fully consent for the participation of my child/ward in the above study.

Signature of the parent/ LAR: _____ Date: _____

Signature of the investigator: _____ Date: _____

ASSENT FORM

(for children below 18 years of age)

Assent form to participate in a research

Child Participant's name: Date of birth/Age:

Parent/LAR' s name: Address:

Title of the Resaerch:

The purpose of the study have been provided to me in writing and explained to me in my own language. I confirm that I have understood the above study and had the opportunity to ask questions. I understand that my participation in the study is voluntary and that I am free to withdraw at any time, without giving any reason. I agree not to restrict the use of any data or results that arise from this study provided such a use is only for scientific purpose(s). I understand that following completion of study as well as during publication of the results, confidentiality of my identity will be maintained. I fully assent to participate in the above study.

Signature of the child participant : Date:

Signature of the Investigator : Date:

CONSENT FORM

Title of the Research:

Participant's name: Address:

I…… voluntarily agree to participate in this research study. I understand that even if I agree to participate now, I can withdraw at any time or refuse to answer any question without any consequences of any kind. I understand that I can withdraw permission to use data from my interview within two weeks after the interview, in which case the material will be deleted. I have had the purpose of the study explained to me in writing and I have had the opportunity to ask questions about the study. I agree for this interview to be tape-recorded. I understand that the audio recording made of this interview will be used only for analysis and that extracts from the interview, from which I would not be personally identified, may be used in any conference presentation, report or journal article developed as a result of the research. I understand that no other use will be made of the recording without my written permission, and that no one outside the research team will be allowed access to the original recording. I understand that all information I provide for this study will be treated confidentially. I fully consent to participate in the above study.

Signature of the participant: _____ Date: _____

Signature of the investigator: _____ Date: _____

CONSENT FORM (for participants less than18 years of age)

Parent/Legally acceptable representative (LAR)

Title of the Research:

Participant's name: Address:

Parent/LAR's name:

The purpose of the study have been provided to me in writing and explained to me in my own language. . I confirm that I have understood the above study and had the opportunity to ask questions. I understand that my child/ward's participation in the study is voluntary and that I am free to withdraw my child/ward at any time, without giving any reason. I understand that I can withdraw permission to use data of my child/ward's interview within two weeks after the interview, in which case the material will be deleted. I agree for my child/ward's interview to be tape-recorded. I understand that the audio recording made of this interview will be used only for analysis and that extracts from the interview, from which I would not be personally identified, may be used in any conference presentation, report or journal article developed as a result of the research. I understand that no other use will be made of the recording without my written permission, and that no one outside the research team will be allowed access to the original recording. I understand that all information my child/ward provide for this study will be treated confidentially. . I fully consent for the participation of my child/ward in the above study.

Signature of the parent/ LAR: _____ Date: _____

Signature of the investigator: _____ Date: _____

ASSENT FORM

(for children below 18 years of age)

Assent form to participate in a research

Child Participant's name: Date of birth/Age:

Parent/LAR' s name: Address:

Title of the Research:

The purpose of the study have been provided to me in writing and explained to me in my own language. I confirm that I have understood the above study and had the opportunity to ask questions. I understand that even if I agree to participate now, I can withdraw at any time or refuse to answer any question without any consequences of any kind. I understand that I can withdraw permission to use data from my interview within two weeks after the interview, in which case the material will be deleted. I have had the purpose and nature of the study explained to me in writing and I have had the opportunity to ask questions about the study. I agree for this interview to be tape-recorded. I understand that the audio recording made of this interview will be used only for analysis and that extracts from the interview, from which I would not be personally identified, may be used in any conference presentation, report or journal article developed as a result of the research. I understand that no other use will be made of the recording without my written permission, and that no one outside the research team will be allowed access to the original recording. I understand that all information I provide for this study will be treated confidentially. I fully assent to participate in the above study.

Signature of the child participant : Date:

Signature of the Investigator : Date: